

I hereby certify that this paper and/or fee is being deposited with the United States Postal Service "EXPRESS MAIL POST OFFICE TO ADDRESSEE" service under 37 CFR 1.10 on the date indicated below and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231

Signature

Date

Express Mail Label No.: 326 715 643 US

Inventors: Randall Scott Springfield and Wayne Freeman

METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

FIELD OF THE INVENTION

The present invention relates to computer systems, and more particularly to a method and system for ensuring that the computer system boots from a trusted source.

BACKGROUND OF THE INVENTION

Figure 1 depicts a conventional computer system 10. The computer system 10 includes a processor 12 that runs an operating system 14 for the conventional computer system 10. The conventional computer system 10 also includes a bridge 16 that provides an interface between the processor 12 and other certain components. In particular, the bridge 16 is typically a southbridge that connects the processor 12 with a bus, such as a PCI bus, having one or more connectors 18. The computer system 10 also includes a FLASH boot source 20, coupled with the processor 12 typically through the bridge 16. When the conventional computer system 10 boots up, the FLASH boot source 20 is typically used as the boot source for the processor 12. Once the BIOS has been loaded through booting, the computer system 10 can function normally.

Although the conventional computer system 10 functions in general, one of ordinary skill in the art will readily recognize that the conventional computer system 10 is subject to attack. Although the computer system 10 normally uses the FLASH boot source 20, it is possible to circumvent the FLASH boot source 20 by placing another boot source at the PCI connector 18. If a PCI boot source (not explicitly shown in Figure 1) is placed at the PCI connector 18, the PCI boot source would be used instead of the FLASH boot source 20. Thus, the computer system 10 would have the BIOS loaded from another, unknown or unwanted boot source. Consequently, an unscrupulous individual could attack the conventional computer system 10. The conventional computer system 10 could be adversely affected by the unknown boot source.

Because the boot source for the conventional computer system 10 can be unknown, the conventional computer system 10 does not have a trusted boot source. A trusted boot source is a boot source that is known and can be verified. A trusted boot source is desired to comply with security requirements, such as those formulated by the trusted client platform association ("TCPA"). It is, therefore, desirable to ensure that the conventional computer system 10 has a trusted boot source. In particular, it would be desirable for the FLASH boot source 20 to be a trusted boot source for the conventional computer system 10.

One mechanism for ensuring that the conventional computer system 10 has a trusted boot source is to preclude the conventional computer system 10 from ever booting off of any source coupled to the PCI connector 18. However, during manufacturing, the FLASH boot source 20 is typically placed into the conventional computer system 10 prior to being programmed. The conventional computer system 10 is then typically booted off of a boot source (not shown) coupled to the PCI connector 18 so that the FLASH boot source 20 can

be programmed in place. Preventing any booting from a source connected to the connector 18 would preclude the FLASH boot source 20 from being programmed in place and would alter the way manufacturers must assemble the computer system 10. Consequently, such a solution would be undesirable.

Accordingly, what is needed is a system and method for ensuring that the boot source for the computer system is a trusted boot source. The present invention addresses such a need.

SUMMARY OF THE INVENTION

The present invention provides method and system for evaluating a boot source in a computer system having a processor. The method and system comprise determining the boot source used by the processor each time the computer system boots and allowing the boot source to be specified once as a known boot source. The boot source is determined by storing an identity of the boot source in a first register. The boot source can be specified once as the known boot source in a second register. The registers are preferably in a bridge coupling the processor to the known boot source.

According to the system and method disclosed herein, the present invention provides a mechanism for ensuring that the boot source is a trusted, known boot source, preferably a FLASH boot source, and checking the boot source to ensure that a trusted source, preferably the FLASH boot source, has been used.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a conventional computer system.

Figure 2 is a block diagram of a computer system including a system in accordance with the present invention for providing a trusted boot source.

Figure 3 is a high-level flow chart of a method in accordance with the present invention for providing a trusted boot source.

Figure 4 is a more detailed flow chart of a method in accordance with the present invention for providing a trusted boot source.

DETAILED DESCRIPTION OF THE INVENTION

The present invention relates to an improvement in computer system. The following description is presented to enable one of ordinary skill in the art to make and use the invention and is provided in the context of a patent application and its requirements. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the generic principles herein may be applied to other embodiments. Thus, the present invention is not intended to be limited to the embodiment shown, but is to be accorded the widest scope consistent with the principles and features described herein.

The present invention provides method and system for evaluating a boot source in a computer system having a processor. The method and system comprise determining the boot source used by the processor each time the computer system boots and allowing the boot source to be specified once as a known boot source. The boot source is determined by storing an identity of the boot source in a first register. The boot source can be specified once as a known boot source in a second register.

The present invention will be described in terms of a particular computer system having a certain arrangement of components. However, one of ordinary skill in the art will

readily recognize that this method and system will operate effectively for other computer systems having different components or a different arrangement of components.

To more particularly illustrate the method and system in accordance with the present invention, refer now to Figure 2, depicting one embodiment of a computer system 100 utilizing a system 150 in accordance with the present invention for providing a trusted boot source. The computer system 100 thus includes a processor 110 capable of running an operating system 112. The computer system 100 also includes a bridge 120, a connector 130 and an internal boot source 140. For clarity, only a portion of the computer system 100 is depicted. Additional or different components could be used in the computer system 100. The bridge 120 couples the processor 110 with the internal boot source 140 and the connector 130. The bridge 120 could also couple the processor with other components, such as a PCI bus or a USB hub (not shown). The bridge 120 is preferably a southbridge, but could be another bridge. The connector 130 is preferably a PCI connector, but could be another type of connector. The connector 130 can thus be used to connect the computer system 100 to a boot source (not shown) to program the FLASH boot source 140 in place during manufacturing.

The system 150 is shown as being placed in the bridge 120. However, in an alternate embodiment, the system 150 could be placed in another portion of the computer system 100. The system 150 preferably includes a first register 152 and a second register 154. The first register 152 is preferably a read only register that can only be read by the operating system 112. The first register 152 is preferably written to during each boot of the computer system, as described below. However, in a preferred embodiment, the second register 154 can only be written to once.

The first register 152 preferably stores the identity of the boot source used by the computer system 100 for the most recent boot. In a preferred embodiment, the first register 152 performs this function by reporting the source of the first one hundred instructions performed during booting. Thus, the identity of the boot source used by the computer system 100 can be verified by querying the first register 152. The second register 154 stores the identity of a known boot source which the computer system 100 is to use for booting. Preferably, the known boot source whose identity is stored in the second register 154 is to be used for the next boot. Once this identity is written to the second register 154, preferably during manufacturing, all subsequent boots will be from the known boot source. In a preferred embodiment, this known boot source is the FLASH boot source 140. Thus, the system 150 allows for a known, trusted boot source to be provided.

Figure 3 is a high-level flow chart of a method 200 in accordance with the present invention for providing a trusted boot source. The method 200 is preferably used in conjunction with the system 150 of the computer system 100 depicted in Figure 2. Consequently, the method 200 will be described in conjunction with the computer system 100. Referring to Figures 2 and 3, the boot source to be used by the computer system 100 is specified, via step 202. In a preferred embodiment, step 202 includes writing the identity of the FLASH boot source 140 to the second register 154 a single time. This preferably occurs during manufacturing. As described above, the second register 154 stores the identity of the boot source to be used for the next boot. Thus, once the identity of the FLASH boot source 140 has been stored in the second register 154, the FLASH boot source 140 will be used for all subsequent boots. The identity of the boot source actually used by the computer system 100 in booting up is determined, via step 204. In a preferred embodiment, step 204 includes

providing the identity of the source of the first one hundred instructions to the first register 152.

Thus, the method 200 provides a trusted boot source for the computer system 100. When the identity of the FLASH boot source 140 is written to the second register 154, the FLASH boot source 140 is ensured to be the boot source for the computer system 100. Furthermore, the actual boot source used is reported using the first register 152. The use of the FLASH boot source 140 can thus be confirmed by querying the first register 152. Thus, the boot source for the computer system is known (due to the second register 154) and can be verified (using the first register 152). The method 200, therefore, can provide a trusted FLASH boot source 140 for the computer system 100.

Figure 4 is a more detailed flow chart of a method 250 in accordance with the present invention for providing a trusted boot source. The method 250 is preferably used in conjunction with the system 150 of the computer system 100 depicted in Figure 2. Consequently, the method 250 will be described in conjunction with the computer system 100. Referring to Figures 2 and 4, the identity of the known boot source to be used by the computer system is written a single time to the second register 154, via step 252. Because the second register 154 is a write once register, the boot source written to the second register 154 will be used for all future boots of the computer system 100. In a preferred embodiment, the known boot source written to the second register 154 is the FLASH boot source 140. Each time the computer system 100 boots, the identity of the boot source is written to the first register 152, via step 254. Preferably, step 254 includes providing the identity of the source of the first one hundred instructions executed by the computer system 100 to the first register 152. Because the first register 152 is a read only register, the operating system 112

or other portion of the computer system 100 does not overwrite the identity of the boot source actually used and reported by the first register 152. The operating system then checks the identity of the boot source actually used, via step 256. The operating system queries the first register 152 and can compare the identity stored in the first register 152 to the identity of the FLASH boot source 140. Based on this comparison, the computer system 100 takes appropriate action, via step 258. If the contents of the first register 152 and the second register 154 match, then the computer system 100 continues with normal operation in step 258. If, however, it is determined that the boot source used is not the same as the known boot source indicated in the second register 154, then the computer system 100 may shut down or take other action in step 258.

Thus, the computer system 100 and the method 200 and 250 provide a trusted boot source that is preferably the FLASH boot source 140. The known boot source to be used is specified, preferably in a write once register 154. In addition, the computer system 100 and the methods 200 and 250 can verify the identity of the boot source actually used by the computer system 100, preferably through the use of the first register 152. As a result, a trusted boot source is provided for the computer system 100. This goal is achieved without precluding the FLASH boot source 140 from being programmed in place. Prior to specifying the known boot source to be used in the second register 154, the computer system 100 can boot from a boot source (not shown) coupled to the connector 130. Thus, a trusted FLASH boot source 140 may be provided for the computer system 100 without requiring a significant change in manufacturing of the computer system 100.

A method and system has been disclosed for providing a trusted boot source for a computer system. Although the present invention has been described in accordance with the

embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations to the embodiments and those variations would be within the spirit and scope of the present invention. Accordingly, many modifications may be made by one of ordinary skill in the art without departing from the spirit and scope of the appended claims.

100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000